CommandCenter® Secure Gateway

(Ver 3.1.0)

Questions	Answers
What is CommandCenter Secure Gateway (CC-SG)?	CommandCenter Secure Gateway (CC-SG) is a management appliance that provides unified, secure access to KVM, serial, and power ports of data center devices via a web browser. Compatible with Raritan's Dominion® Series, Paragon, IP-Reach® and CommandCenter NOC, CC-SG provides policy and security management of users and devices connected to Raritan's products, other embedded solutions like HP iLO/RILOE, IPMI, Dell DRAC, IBM RSA, as well as, other in-band software solutions such as RDP, VNC, and SSH.
What are the different CC-SG hardware options available?	Raritan offers different hardware versions to address both small and medium size businesses as well as large enterprises with thousands of servers and other IT appliances. CC-SG E1 is targeted at large deployments as well as environments where dual power supply is required for redundancy. The CC-SG V1 is a powerful KVM and in-band access and power management appliance designed to address network redundancy or subnet proxy environments. For more information visit Raritan.info.
Why would I need CC-SG?	As you deploy more data center servers and appliances, IT management becomes increasingly complex. CC-SG allows an IT administrator to access, manage and view all equipment, and users, and to access permissions from a single remote device.
Which Raritan products does CC-SG support?	CC-SG is able to manage analog KVM switches and digital appliances, including Raritan's Dominion KX KVM-over-IP switches, Dominion SX serial-over-IP console servers, Dominion KSX remote office appliances, and CommandCenter NOC. With Paragon II System Controller (P2-SC), multiple Paragon II switches and the servers that are connected to these switches can be accessed and controlled with CC-SG. P2-SC also provides single sign-on, and centralized authentication and authorization of remote Paragon II users and enables administrators to centrally perform administrative functions on Paragon II switches.
How does CC-SG integrate with other Raritan products?	CC-SG uses a powerful proprietary search and discovery technology that identifies and connects selected Raritan devices. Once CC-SG is connected and set up, device connection is transparent and administration is simple.
Is the status of CC-SG limited by the status of the devices that it proxies?	No. CC-SG software resides on the dedicated appliance. This means that even if the device being proxied by CC-SG is not operating, you will still be able to access CC-SG.
Can I upgrade to newer versions of CC-SG as they become available?	Yes. Information about firmware availability or firmware may be downloaded from the Raritan website at http://www.raritan.info/support/sup_upgrades.aspx Upgrades are done through CommandCenter Secure Gateway's client Graphical User Interface. Additionally, the CC-SG appliance has a CD/ROM drive to facilitate install/upgrades.

Questions	Answers
How many login accounts can be created for CC-SG?	There is no specified limit to the number of login accounts that can be created. However, licensing restrictions or system specifications will limit the number of concurrent users or the number of nodes associated with the CC-SG based on the configuration deployed.
Can I assign specific node access to a specific user?	Yes, if you have Administrator permissions. Administrators have the ability to assign specific nodes per user.
How are passwords secured in CC-SG?	Passwords are encrypted using MD5 encryption, a one-way hash. This provides additional security to prevent unauthorized users from accessing the password list.
Is there any way to optimize the performance of Microsoft Internet Explorer for CC-SG?	To improve the performance of Microsoft® Internet Explorer® (IE) when accessing the CC-SG console, select Tools > Internet Options > Advanced from the main IE menu bar. Scroll down and disable (uncheck) the "JIT compiler for virtual machine enabled," "Java logging enabled," and "Java console enabled" options. For compatibility of specific browser versions refer to the CC-SG Compatibility Matrix at www.raritan.info/support
Why do I receive a "No longer logged in" message when I click on any Menu in CC-SG after leaving my workstation idle for a period of time?	CC-SG times each user session. If there is no activity for a pre-defined period of time, CC-SG logs the user out. The time period is pre-set to 30 minutes, but can be reconfigured. It is recommended that users exit CC-SG when they finish an operation.
An administrator added a new node to the CC-SG database and assigned it to me, but I cannot see it in my Device Selection table. Why?	Newly added nodes should automatically appear in the user's node table. To update the table, and see the newly assigned node, click the [Refresh] button. *Note: Clicking refresh on the CC-SG toolbar will not close the session. Only the browser refresh button will close the session.*
The event times in the Audit Trail seem incorrect. Why?	Event times are logged according to the time settings of CC-SG clock. CC-SG time settings may be different from your PC client time settings because of either different time zone or daylight savings time settings. You can modify the clock by logging into CC-SG and accessing the Time/Date tab under Configuration Manager.
Which version(s) of Java does CC-SG support?	For the server side, CC-SG supports Java® 1.4.0 and later versions. On the client side, CC-SG supports Java 1.4.2 and later versions. You need to download the Java 2 plug-in if using Internet Explorer. Netscape® by default will use the Sun® JVM. Please check the Application Notes, available on the Raritan website at http://www.raritan.info/support/sup_prdmanuals.aspx for your release to confirm supported versions.
If there are more than 1000 users, how would this be managed, e.g., support for Active Directory® (AD)?	CC-SG works with Microsoft Active Directory (AD), Sun iPlanet™ or Novell® eDirectory™. If a user account already exists in an authentication server then CC-SG supports remote authentication using AD, TACACS+, RADIUS, LDAP or LDAP(S) authentication. CC-SG also supports remote authorization for AD.
Can customers also have root access for auditing and accountability?	Yes. Customers can have root access.

Questions	Answers
What is the impact on other usage that would be blocked through the active usage of the console port?	A console is generally considered a secure and reliable access path of last resort. Some UNIX systems allow root login only from the console. For security reasons, other systems might prevent multiple logins, so that if the administrator is logged in from the console, other means of access are denied. In addition, from the console, the administrator can also disable the network interfaces when/if necessary to block all other access.
What is the bandwidth usage per client?	Remote access to a serial console over TCP/IP is about the same level of network activity as a telnet session. However, it is limited to the RS232 bandwidth of the console port itself, plus SSL/TCP/IP overhead. The Raritan Remote Client (RRC) controls remote access to a KVM console. This application provides tunable bandwidth from LAN levels down to a level suitable for a remote dial-up user. Using direct mode on CC-SG the bandwidth usage is between the CC-SG client and the device, not the CC-SG server.
Specifically what type of changes can a management system monitor and alert on?	CC-SG will log user activity (login/logout, connect/disconnect) and configuration changes at both CC-SG and managed Raritan appliances, and status changes of the connected appliances. All of the above can be forwarded to a network management system or enterprise notification system via SNMP or syslog.
What is the recommended use of Computer Interface Modules (CIMs) being moved / swapped at the physical level with changes to the logical database?	Each CIM includes a serial number and a target system name. Raritan systems devices assume that a CIM remains connected to its named target when its connection is moved to another switch. This move is automatically reflected in the system configuration and is propagated to CC-SG. If the CIM is moved to another server, an administrator must rename the CIM.
How does CC-SG integrate with Blade Chassis products?	CC-SG can support any device with a KVM or serial interface as a transparent pass-through. All blade chassis come with one KVM connection for the management of the blade system. Some blade servers allow KVM connections on a blade basis through a proprietary add on connector from the blade server manufacturer. This would allow access and control of the blade server through Raritan devices. In addition, CC-SG can incorporate access and power management through embedded cards such as iLO/RiLOE . Typically, these cards are located on the blade chassis and control the whole enclosure. CC-SG also provides power management through power strips connected to Raritan devices. CC-SG can also provide centralized access to individual blades with RDP, VNC, or SSH.
What options are available for authentication with directory services and security tools, e.g., LDAP, AD, Radius, etc.?	CommandCenter Secure Gateway permits local authentication as well as remote authentication. Supported remote authentication servers include: • AD • TACACS+ • RADIUS • LDAP
Will the current Paragon solution work with CC-SG?	Raritan has introduced an interface device – Paragon II System Controller (P2-SC) -- that integrates Raritan's Paragon II analog Cat5 KVM switches with CC-SG. To find out more about the Paragon II System Controller go to www.raritan.info/paragonII

Questions	Answers
For the leaf nodes (Raritan devices managed by CC-SG) how will I know if someone else is logged in?	CC-SG presents the list of users logged in to a leaf device and can show which users are currently accessing a node through the active users report. In addition, a bold interface to a node would indicate that it is currently being accessed by a user.
Does CC-SG have the ability to look at multiple device screens? How is this presented?	If there are many devices connected to CC-SG, you can scroll through the screens to view them all. You will be able to open many screens; each one corresponding to one node, but you will be restricted on the KVM side by the capacity of the KVM-over-IP channels.
Is SSL encryption internal (LAN) or external (WAN)?	Both. The session is encrypted regardless of source, i.e. LAN/WAN.
Can audit/logging abilities track down to who switched a power plug on/off?	Direct power switch off is not logged, but the power on -off through the CC-SG GUI is recorded in the audit trail and can be viewed in Audit Trail report.
Does CC-SG support Client Certificate Request?	Yes. Under CC-SG, navigate to Security Manager under Setup.